Cyber Threat Intelligence for Improving Cyber Supply Chain Security

Abel Yeboah-Ofori
Sch of Arch, Computing & Eng.
University of East London
London, E16 2RD, UK
u0118547@uel.ac.uk

Shareeful Islam
Sch. of Arch, Computing & Eng.
University of East London
London, E16 2RD, UK
shareeful@uel.ac.uk

Ezer Yeboah-Boateng
Faculty of Informatics
Ghana Technology University College
PMB100, Accra. Ghana
eyeboah-boateng@gtuc.edu.gh

Abstract: **Cyber supply chain (CSC) systems provide operational efficiency and business continuity due to the integrated nature of various network system nodes. Such integration has made the overall system vulnerable to various cyber attacks and malware propagation is one of the common attacks for CSC. Cyber threat intelligence (CTI) provides an organization the capability to identify, gather, analyze threats and the associated risks so that CSC organization can forecast the existing and future threat trends and manage the cybersecurity risk in a proactive manner. A threat actor may attack the system and propagate a malware. The purpose is to manipulate, alter, or change delivery mechanisms. It is imperative to integrate CTI into the existing cybersecurity practice to detect and understand the threat actor's intents and motive. In our previous paper, we used threat analysis gathering to provide us an understanding of the adversaries' capabilities, actions, and intents. This paper contributes to improving the cybersecurity of CSC by using CTI. In particular, we extend our previous work which identifies and analysis CSC attacks and adopts CTI approach to understand the attack trends so that appropriate control can determine proactively. We use the malware a smart grid case study as CSC context to demonstrate our approach. The result demonstrations how CTI approach is applied to assist in preventing cyberattacks and to disseminate threat information sharing.**

Keywords: Cyber Threat Intelligence, Cyber Supply Chain, Tactics Techniques Procedure, Cyber Security, Threat Moddeling

I. INTRODUCTION

Cyber supply chain (CSC) is a network of various organizational components connected together with other vendors, suppliers, and consumers for business processes, goals, and objectives [1]. CSC systems are more prone to cyber-attack as they are vulnerable, and any attack can cascade from one affected node to other nodes. CSC attacks have increased exponentially and have impacted greatly on private and government organizations. There are many examples of successful cyber attacks such as Dragonfly a Cyber Espionage group 2011 [2], known for targeting companies through their supply chain [2]. Shylock Banking Trojan 2014: Man in a Browser attack. Compromise legitimate electronic banking e-products and e-process services websites through a website builder used by creative and digital agencies [2]. Saudi Aramco cyberattack 2017, an electric grid was halted from operation by cyber attackers at the Saudi Aramco power station [3]. Ukraine power grid attack 2016 [4]. These attacks are sophisticated and organized by multiple attackers. It is necessary to understand these attacks before implementing any effective CTI and control.

Cyber Threat Intelligence (CTI) provides an organization with the capability to undertake the actionable decision with the aim of preventing the attack. The purpose of CTI is to provide evidence-based knowledge relating to the attacker's motives, tactics, and indicators of compromise which helps organizations anticipate future threats and plan controls. Factors such as known-known attacks, Known-Unknown attacks and Unknown-Unknown attacks that are impacting on the evolving threat landscapes and affecting the CSC [5]. Known-known attacks include changing the threat landscape and evolution of smart systems are such as advanced persistent threats. Cascading threat impacts on supply inbound and outbound supply chains that cause known- unknown such as malware attacks and inability to determine the extent of their effects on the CSC. Complex integrations of CSC that has caused unknown-unknown threats such as command and control.

The main contribution of this paper is to improve cybersecurity practices on CSC by using cyber threat intelligence. We integrate concepts from the CSC with CTI so that CTI can support security activities for the cyber supply chain using a systematic process. Finally, we recommend controls based on the CTI information so that CSC organization can improve its overall cybersecurity practice.

II. RELATED WORKS

This section provides an overview of the related works on CSC security, recent cyber attack and CTI approaches that are currently being used in the industries.

A. Cyber Supply Chain Security

CSC security focuses on mechanisms put in place to control and manage cyber attacks to ensure business continuity. NIST proposed three principles of best practices that an organization should develop for defense from the premise that the system will be breached [1]. Woods and Bochman 2018, reviewed the significance of how software component errors built into products in the design or implementation phase causes flaws and CSC attacks [3]. Abel and Islam, 2019, proposed a method that contributes to modeling and analyzing CSC attacks and cyber threat reporting [6]. Reed et al 2017, proposed a framework and catalog of supply chain attack patterns on the CSC system [7].

978-1-7281-7417-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSIoT47925.2019.00012

B. *Cyber attack*

There are numerous examples of successful cyber attacks. Third Party Data Store Attack 2013: A small botnet was observed exfiltrating information [2]. Havex malware 2014, targeted energy sector companies by spreading malware called 'Havex' through several supply chain vectors. [2]. Watering Hole attack: The adversary uses a Remote Access Trojan (RAT) to target a website of an organization supply chain system [8]. Wanna Cry Ransomware attack 2017, infected several companies and energy sectors companies worldwide [9].

C. *Cyber Threat Intelligence*

The goal of CTI is to provide information about the technical indicators, context, motivation, and actionable advice relating to the existing and emerging threat. ENISA 2018, propose strategic CTI goals that support executives in decision making, operational goals that provide an understanding of the threat actors modus operands, intents, and TTPs, then tactical goals into concrete detection capabilities [5]. MITRE 2013, pull together a comprehensive set of data sources system security engineering to provide a holistic view of supply chain attacks of malicious insertion and generated a catalog of attack patterns for risk management purposes [10]. Friedman & Buchanan, proposed CTI approach based on the organizational intelligence requirements, collect information, analyses and disseminate to protect assets and documents. The process includes developing [11]. Zane Pokorny 2018, proposes a CTI lifecycle approach that includes direction, collection, process, analysis, and dissemination required to identify intelligence goal [12].

Scott et al 2019, demonstrated the stages of network-based vulnerabilities, attack, methods on supply chain systems and applied the concepts of kill chain including countermeasures [13]. NERC, 2017, developed an objective based on reliability standards that realistically address the reliability gaps in CSC security process [14]. CAPEC proposed attack patterns that focus on disruption of supply chain lifecycle through the manipulation of the software, hardware, and services during product manufacturing and distribution [15].

ENISA 2018 proposed strategic CTI goals that support executives in decision making [5]. Further, MITRE 2013 proposed software security engineering concepts for CSC attacks [10]. Additionally, Zane Pokorny 2018 proposed a CTI lifecycle approach required to identify intelligence goals [12]. Similarly, Scott et al 2019 proposed to kill chain concepts for CSC vulnerabilities and attacks [13]. However, none of the authors identifies and analysis CSC attacks and adopts CTI approach to understand the attack pattern, TTPs, and trends from smart grid CSC organizational context.

III. Integration of CTI for CSC

Integrating CTI in CSC systems has become integral due to factors such as an increase in the use of a sophisticated cyber physical system (CPS). The proposed approach considers CTI core cyber threats concepts such as indicators, TTPs, incident, and threat actors and links them with CSC concepts such as goal, inbound and outbound supply chains. It also includes a process to analyze the cyber threat.

A. *Why CTI is Important for CSC*

CTI is relevant for CSC as it provides detailed knowledge and understanding of the threat actor's motives and intent required to implement CSC security. Further, the globalized and distributed nature supply chain systems have made it significant to include CTI in CSC. Additionally, the complex, logical and relational entities involved in the CSC network systems developments lifecycle as well as the number of channels or vendors that handle this product and services before it gets to the final customer are also factors. Thus, without the required integration of CTI lifecycle approach into CSC development, it will be highly unlikely to effectively mitigate the attacks, risks, vulnerabilities, and exploits that are currently prevailing on CSC systems.

B. Proposed approach

This section uses the CTI approach, process lifecycle and its integration for cyber security analysis of CSC to provide a method of determining the threat intelligence concepts. We use CTI concepts from existing literature [5, 10, 12, 13].

C. *CTI Lifecycle Implementation*

CTI lifecycle implementation Phase and a brief process as below: Direction, Identify, Gather, Machine Learning, Analysis, Evaluate, Controls and Disseminate.

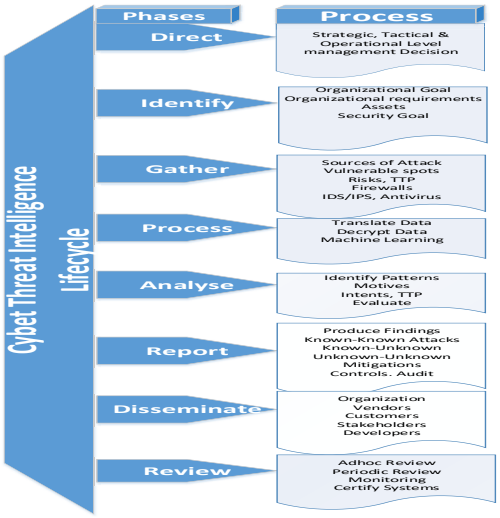

Figure 1. Cyber Threat Intelligence Lifecycle

D. *CTI Phases*

Direct: The direction phase requires that the organization strategic, tactical and operational management come together to decide on CTI goals and

objectives. Further, they must form a CTI strategic management team to oversee the identification, investigations, review, and evaluate the supply chain system processes and applications. The objectives include: Assign a CTI lead manager, Identify security goals to inform proper CSC security controls.

Identify: The identification process includes identifying all the organizational goal, CSC requirements, assets, supply chain network nodes, IP address, technical threats, and human threats.

Gather: The gathering process involves gathering sources of attacks, vulnerable spots, risks TTPs. The data are gathered from firewalls logs, collecting a signature, threat indicators and events from IDS/IPS, antimalware from the various endpoints. We expound on TTP and threat indicators as follows: Tactics, Techniques, and Procedures (TTP) is a representation of the behavior or modes of operations of the adversary [16].

- Tactics: Includes how the adversary carries out reconnaissance for initial intelligence gathering. Tactics may be to use redirect victims to a compromise electronic banking e-products and e-process service website to gain access into the supply chain system.
- Techniques: are the tools, skill, and capabilities deployed. Use social engineering technique and send a spear phishing email or attach a redirect script into a website software so that whenever the victims download and install, it open and provide access to the adversary.
- Procedures: are uniquely used a set of tactics and techniques for an attack. Procedures may vary depending on the threat actor's goal, motive, purpose, and intent. The advance actor may deploy highly sophisticated procedure such as APT.

Process: Translating data into meaningful information and use decryption tools for hashing functions. This includes analyzing IDS/IPS logs, firewall logs, and Antimalware intrusions predict attacks that could be fed into the CTI. These assist in determine false positives and false negative rates alert on the dataset and accurate predictions.

Analysis: The process includes analyzing the Identify attack patterns, motives, and intents to understand TTPs. Analyze the logs, alerts, to understand the attack trends as identified in the initial process. This includes identifying what happened, how, why, when, who and where on the CSC system.

Evaluate the threats, risks, and impacts on CSC. Formulate an understanding of the effects on business process, organizational goal and the financial impact and for budgeting. Additionally, we use a cost benefit analysis to determine the cost of alternatives.

Report. This phase reports on the findings of the analysis and evaluations for strategic management decision makings. It determines the Known-known attacks, Unknown-Unknown, and Known-Unknown attacks. The process provides a mechanism for control required to ensure strategic management decisions to mitigate these treats. Additionally, it is used for third party auditing purposes, configurations, and conformance.

Disseminate: The process includes how CTI information is shared to various organization, institutions, vendors and businesses on the CSC system. It designates information and creates awareness on the various alerts, how to assess and monitor threats, risk, and control. Additionally, system developers could use the information for software developments purposes.

Review: The review phase requires management to hold ad-hoc, periodically and annual security meetings to monitor security threats, understand the threat landscape and ensure the systems are certified. These ensure information assurance and situational awareness.

These CTI lifecycle and reports approach to inform the required strategic, tactical and operational security decision-making and controls that must be implemented in the relevance of the CTI.

IV. DETECTING CTI USING ATTACK PATTERNS, VECTOR AND TTP

Due to the lack of visibility of cyber threats and the phenomenon surrounding its impacts, it is imperative that we model the attack lifecycle to inform our CTI lifecycle. This section considers attack pattern, prerequisites, vectors, TTP and indicators as properties in realizing CTI for CSC security goal.

The attack pattern has a prerequisite as a property that provides the adversary the necessary information after carrying out reconnaissance to determine whether the system is exploitable or not. This information could assist us in carrying out supply chain risk assessments. For instance, the adversary could gain access when the following vulnerabilities exist in the supply chain system:

- The supply chain variables are accessible to the threat actor due to poor constraints and server misconfigurations on the CSC system.
- The business applications used for the supply chain variables could be exploited through the use of incorrect user data.
- Information retrieved through inputted data is not configured properly due to poor validation.
- The variables are not well encapsulated to prevent software redirect. For instance, setting an input variable as public in a class when developing the software source codes makes the website open to external attackers

A. CSC Attack Life Cycle

This section follows concepts from 3.1and implements the CTI life cycle process to achieve organizational security goal.

Phase 1: The organizational goal is to adopt a CTI approach to identify attack patterns, TTPs and threat indicators. This includes the executive summary of organizational goal, identification of assets, strategic objectives, and assigning security team/lead to oversee the implementation of CTI lifecycle as in (Direct Phase).

Phase 2: The attacker goal is to abort the security goal by using Malware, SQL injection, XSS or session high jacking attacks to penetrate the system to manipulate or cause DoS attacks. In the identification phase, the security team identifies the CSC system vulnerabilities, risks, and attacks that could impact the assets and supply chain system. This includes using TTPs to determine the attacker goal. The figure below explains how we model the CSC attack life cycle:

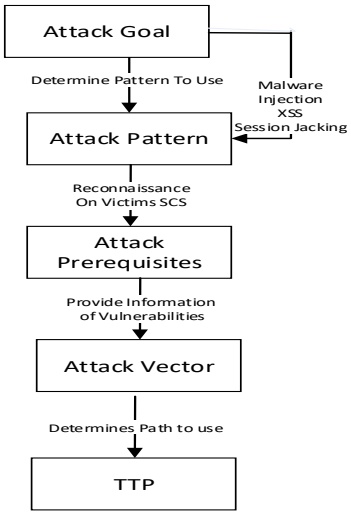

Figure 2. Supply Chain Attack Life Cycle

The CTI approach and parameters are used to express an indication of an attack. The attacker goal determines the attack pattern to use e.g. malware, spyware or Injection. Further, the attack pattern determines the prerequisites required after carrying out reconnaissance on the victim's system to determine if an attack will be successful. The perquisites determine the attack vectors that will be deployed against the victim. After all these steps have been achieved, then the attacker uses the TTPs which act as a schema for the attacker goal. Implementing the gathering, processing, and analysis in phase 3, 4, and 5 as discussed in 3.1 provides us the processed information required for our threat intelligence gatherings.

B. CTI Indicators for CSC

CTI Indicators are TTP parameters that express that an attack of a certain nature is imminent, in progress or has occurred. We use SCS threat activities, adversary behaviors, risky events, or state of the incident to determine what could serve as an indicator. The CTI indicators provide:

- CSC attack incidents and course of actions
- Nature of cyberattack indicators
- TTPs that were deployed

The CTI Indicators convey specific observable patterns of CSC attacks combined with contextual intelligence that represent threat actor's behavior.

V. CONTROLS

Controls are a security mechanism put in place to mitigate specific cyber threats. The CTI lifecycle, TTP lifecycle, and reports inform the required directive, preventive, detective, recovery and corrective controls. The following provides CSC control.

Table 1. CSC Security Controls and Recommended Standards Reference.

No	Control	Principle	Critical	Security Purpose	Implement	Activity
1	Create Inventory and Control of Hardware Assets	Identify and manage inventory of hardware devices on the network. Give only authorized device access.	Attacker's interest is in devices as which might be out of synch with security updates. E.g. laptops or Bring-Your-Own-Devices (BYOD	New installations that are un-configured and unpatched with appropriate security updates could be exploited	Identify devices connected to the organization's network. Audit and update hardware asset.	Maintain an accurate and up-to-date inventory and audit trail. That identifies assets connected to the supply chain network or not.
2	Create Inventory and Control of Software Assets	Identify and Manage inventory, identify, and correct all software so that only authorized software is installed and execute. Prevent unauthorized and unmanaged devices access	Attackers scan victim's websites for vulnerabilities to remotely exploited. Or distribute hostile web pages and document files, or trustworthy third-party sites.	Control software plays a critical role in planning and executing system backup, incident response recovery	Utilize software inventory tools throughout the organization to automate the documentation of all software.	Utilize application alerts on all assets to ensure that only authorized software executes
3	Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of	The must be CTI gatherings, software updates, patches, security advisories. Understand threat and vulnerabilities. The activity requires time,	Attackers exploit vendors. When a new vulnerability is known. Develop patches or signatures updates, and defenders to	Organizations that do not scan for vulnerabilities and proactively address flaws	Utilize tools to automatically scan systems to identify vulnerabilities. Deploy automated updates provided

		opportunity for attackers.	attention, and resources.	assess risk and patches.	face likelihood of attacks.	by the software vendor.
4	Controlled Use of Administrative Privileges	Not changing the hard-coded password default. Impacts on the processes and tools used to track/control/prevent/correct user, assignment, and configuration of admin privileges.	Misuse of admin privileges is a primary method for attackers to get inside a target system. Technique takes advantage of uncontrolled admin privileges.	Workstation user running as a privileged user is tricked to open a malicious email attachment or website hosting exploit browsers.	Change default hard-coded pwd. Ensure admin user account access use dedicated account for admin activities	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Establish, implement, and actively manage (track, report on, correct) security configuration of mobile laptops, servers, workstations using configuration management and change control process	Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of options and CTI gathering	Updates must be done regularly, Configuration is installed. New vulnerabilities are reported, update software to support new operational requirement.	Maintain documented, standard security configuration standards for all authorized operating systems and software.	Verify security configuration elements, catalog approved exceptions and alert when unauthorized changes occur (SCAP)
6	Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	Deficiencies in security logging and analysis allow attackers to hide their location, software, and activities on victim machines.	Logging records are evidence. Keep audit records for compliance purposes.	Ensure that local logging has been enabled on all systems and networking devices.	Ensure activity logs are aggregated to a central log system for analysis& review

VI. SMART GRID CASE STUDY

We use a case study of a smart grid system that was compromised for our analysis in relation to the CTI approach in section 3. The security team failed to update the software and the adversaries insert malware to exploit that vulnerability to gain access to the control center. Also, the default hard-coded passwords credentials were not changed and that gave the attacker remote access to the network system. For us to the CTI approach to determine the attacks, we first analysis the TTP the attacker deployed on the supply chain system. We use figure 3 below to determine the attack pattern.

- Security Goal: was to implement ad-hoc, periodic and regular software updates on the supply chain system. Change the default-hardcoded password.
- Nature of Attack: Insert malware to exploit the vulnerability and gain access to the system
- Attacker Goal: Take Command & Control and exploit the default hard-coded password to obfuscate.
- Step 1. Reconnaissance: Adversary search online and uses other social engineering methods to gather information e.g. Network Topology, IPs, Software, and Configurations.
- Step 2. Experiment: the adversary uses various attack methods (TTP) and tools to gain control of the victim's systems as intrusion set.
- Step 3. Exploit: compromise the system at this stage and gains access to the systems and determines the attack goal.
- Step 4: Command and Control: adversary uses remote access and APT technics to establish control on the victim CSC system and compromise the default hard-coded password to hide in the systems.

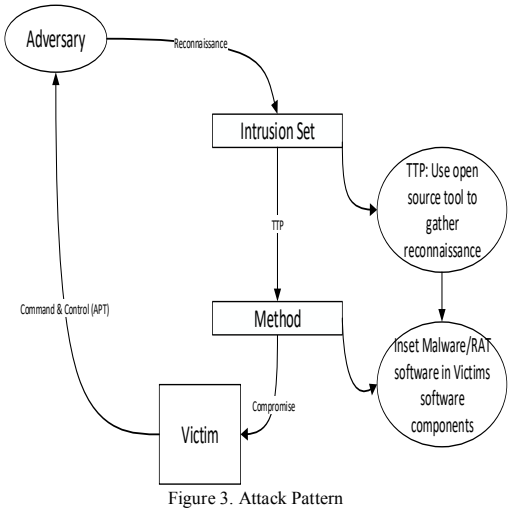

Figure 3. Attack Pattern

A. *Cyber Threat Intelligence Gathering.*

Threat intelligence gathering assists in understand the attacker's mode of operations that includes identifying:

- What is the attacker trying to achieve (Goal)
- What are the capabilities in the form of tactics
- Techniques that they have leveraged overtime

- Procedures that they are likely to leverage

B. Determining Controls Using CTI

We select a particular event such as a malware attack on the smart grid to determine the CTI lifecycle as discussed in section 3.

- Identify all the actors, access rights and privileges
- Carryout vulnerability assessment
- Carryout a Risk Assessment on the supply chain
- Combine probability on attacks with its potential impact on the CSC
- Identify Controls and Standards required to secure the system.

VII. CONCLUSION

Cyber Threat intelligence gathering is a proactive way to assist organizations to gather, analyze and disseminate intelligence, CTI could assist in determining whether an attack could occur in the near future. For instance, if an organization experience 40% of spear phishing or malware attacks after a threat analysis report, we could say that there will be the frequency of attacks in the future. CTI requirements could be used to determine the vulnerability of the system to understand of Known-known attacks, Unknown-Unknown, and Known-Unknown attacks. These are major CSC attacks such as penetration, manipulation, APT and command & control attacks. TTPs consist of the specific adversary behavior exhibited in an attack, it leverages on resources such as tools, infrastructures, capabilities, and personnel. It provides CTI information on the victim's target (who, what or where), that are relevant to exploit targets being targeted. CTI life cycle phase provided us the intended effects, kill chain phases, handling guidance and resources of the TTP information. The CTI gathered will inform the strategic, tactical and operational management roles and responsibilities. Operational level managers could use the CTI indicators, to determine details of attacks and TTPs, relate attacks and provide remediation from the control statement. Tactical level managers could use CTI to feed into the security requirement, validate and prioritize indicators for configuration, auditing, monitoring and escalating threat alerts to the right sources for security products procurements. Strategic level CTI will assist in financial resources allocation, provide a blueprint for executive summary and executive management authorization.

REFERENCES

[1]. J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". NIST Computer. Sec. 2015, 800, 1, doi:10.6028/NIST.SP.800.

[2]. National Cyber Security Centre." Example of Supply Chain Attacks." GCHQ. 2018.

[3]. B. Woods, and A. Bochman, "Supply Chain in the Software Era" Atlantic Council: Washington, DC, USA, 2018.

[4]. K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." 2016.

[5]. C. Doerr, "Cyber Threat Intelligences Standards – A High Level Overview" TU Delft CTI Labs, 2018.

[6]. A. Yeboah-Ofori, and S. Islam. Cyber Security Threat Modeling for Supply Chain Organizational Environments. Future Internet, 2019. 11, 63, doi: 10.3390/611030063

[7]. M. Reed, F. John, and P. Popick, "Supply Chain Attack Pattern: Framework and Catalog. Office of the Assistant Secretary of Defense for Research and Engineering. 2017.

[8]. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX); V1.1, Revision 1; National Cyber Security Centre. "The principles of supply chain security." GCHQ. 2018.

[9]. Controller and Audit General: 2017. Investigation: WannaCry cyber-attack and the NHS. National Audit Office. UK

[10]. MITRE. Threat-Based Defense. Understanding Attackers Tactics and Techniques is Key to Successful Cyber Defense.

[11]. J, Freidman, and M Bouchard. "Cyber Threat Intelligence Guide: Using Knowledge About Adversary to Win The War Against Targeted Attacks." iSightPartners. 2018.

[12]. Z, Porkorny, "What Are the Phases of The Threat Intelligence Lifecycle?" The Threat Intelligence Handbook. A Practical Guide for Security Teams to Unlock the Power of Intelligence. 2018.

[13]. S. R. Nawrocki and T, Baccam, "Cyber Threat to the Bioengineering Supply Chain." Global Information Systems Certification Paper. The SANS Institute. 2019.

[14]. S. Elstein, Noer America Electricity Reliability Corporation. NERC: "Proposed Reliability Standards for Addressing Supply Chain Cyber Security Risk Management." Sept. 2017

[15]. CAPEC-437: Supply Chain. 2018. Common Attack Pattern Enumeration and Classification: Domain of Attack.

[16]. STIX 2.0: Assets Affected in an Incident.